What is claimed is:

1. A method for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, the method comprising:

receiving a secure session establishment request by the second device on the external network to establish a secure communication session with the first device on the internal network;

forwarding the secure session establishment request to the first device;

monitoring the internal network for an approval or disapproval acknowledgement by the first device for the secure session establishment request; and

if an approval authentication acknowledgement is monitored, then configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary.

2. The method of claim 1, further comprising:

determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

3. The method of claim 2 wherein the presence advertisement is delivered in accordance with the UPnP Simple Service Discovery Protocol (SSDP).

4. The method of claim 1, further comprising:

receiving network traffic from the second device corresponding to the second device requesting a UPnP Device Description Document from the first device.

5. The method of claim 1, further comprising:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining the service request identifies a service advertised by the first device in a device description document; and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port.

6. The method of claim 1, further comprising:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device.

7. The method of claim 6, wherein the indicia is a selected one of a globally routable Internet Protocol (IP) address, or an internal network address non-routable on the external network.

8. The method of claim 1, wherein communication within the internal network is in accord with an IPv6 compatible Internet Protocol (IP).

9. The method of claim 1, further comprising:

retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

10. The method of claim 1, further comprising:

receiving network traffic from the second device corresponding to a previous secure communication session established when the second device was previously on the internal network; and

responding to said network traffic with an error such that the second device attempts to re-establish a secure communication session from the external network.

11. The method of claim 1, further comprising:

establishing the end to end secure session connection between the first device on the internal network and the second device of the external network in a single end to end secure session connection between said first and second devices.

12. A method for communicating with a device by way of an intermediary selectively coupling an external network and an internal network, comprising:

receiving a presence advertisement for the device;

storing a network address associated with the first device;

determining services offered by the device; and

while on the external network, issuing a secure communication initiation request to the device via the intermediary.

13. The method of claim 12, wherein the intermediary is configured to:

forward the request to the device;

monitor for an approval or disapproval authentication acknowledgement to the request; and

configure a filter of the intermediary to allow communication with the device if an approval authentication acknowledgement is received.

14. The method of claim 13, wherein the intermediary is further configured to configure the filter to block communication with the device is a disapproval authentication acknowledgement is received.

15. The method of claim 12 wherein the presence advertisement is received while on the internal network.

16. The method of claim 12, wherein while on the internal network, the method further comprising requesting a description of services offered by the device.

17. The method of claim 16, wherein the description of services is requested from the intermediary.

18. The method of claim 12, wherein while on the external network, the method further comprising requesting a description of services offered by the device.

19. The method of claim 18, wherein the description of services is requested from the intermediary.

20. The method of claim 12, further comprising:

receiving an approval authentication acknowledgement to the request; and responsive to the approval, requesting a service of the device.

21. The method of claim 12, wherein the network address associated with the first device is a globally unique network address having an address portion identifying the intermediary.

22. The method of claim 12, wherein a traveling control point performs the method for communicating with the device.

23. A system of devices communicatively coupled with an internal network and an external network via a gateway, comprising:

a first device, communicatively coupled to the internal network, offering services;

a second device selectively coupled with the internal and external networks, the second device seeking a service of the first device, wherein when requesting the service, said requesting includes sending a secure communication initiation request to the first device to facilitate establishing a secure communication session with the first device; and

an intermediary selectively communicatively coupling the first and second devices, wherein the intermediary is configured to receive a secure communication initiation request from the second device over the external network and forward the request to the first device.

24. The system of claim 23, wherein the intermediary is further configured to monitor the first device for an approval or disapproval authentication acknowledgement for the request, and to configure a filter of the intermediary controlling communication

over the first network from the first device based at least in part on a monitored authentication acknowledgement.

25. The system of claim 23, wherein the first device communicates with the second device in accord with the UPnP Security Protocol.

26. The system of claim 23, wherein the secure communication initiation request corresponds to a UPnP Set Session Key (SSK) request.

27. An article comprising a machine-accessible media having associated data for an intermediary selectively coupling an external network and an internal network to dynamically generate filter rules to facilitate establishing an end to end secure session connection between a first device on the internal network and a second device of the external network, wherein the data, when accessed, results in the intermediary performing:

receiving a secure session establishment request by a second device on the external network to establish a secure communication session with a first device on the internal network;

forwarding the secure session establishment request to the first device;

monitoring the internal network for an approval or disapproval acknowledgement by the first device for the secure session establishment request; and

if an approval authentication acknowledgement is monitored, then configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary.

28. The article of claim 27, wherein the data further includes data, which when accessed, results in the intermediary performing:

determining a presence advertisement for the first device has been received before forwarding the secure session establishment request to the first device.

29. The article of claim 27, wherein the data further includes data, which when accessed, results in the intermediary performing:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining the service request identifies a service advertised by the first device in a device description document; and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port.

30. The article of claim 27, wherein the data further includes data, which when accessed, results in the intermediary performing:

providing the second device with an indicia for use by the second device in establishing a communication link to the first device.

31. The article of claim 27, wherein the data further includes data, which when accessed, results in the intermediary performing:

retrieving an Access Control List (ACL) from the first device, the ACL including an identification of devices authorized to establish communication sessions; and determining based at least in part on the ACL the second device is authorized to establish the secure communication session with the first device before forwarding the secure session establishment request to the first device.

32. An article comprising a machine-accessible media having associated data for communicating with a device by way of an intermediary selectively coupling an external network and an internal network, wherein the data, when accessed, results in a machine performing:

receiving a presence advertisement for the device;

storing a network address associated with the first device;

determining services offered by the device; and

while on the external network, issuing a secure communication initiation request to the device via the intermediary.

33. The article of claim 32, wherein the data further includes data, which when accessed by the machine, results in the machine performing:

receiving the presence advertisement while on the internal network.

34. The article of claim 32, wherein the data further includes data, which when accessed by the machine, results in the machine performing, while on the internal network, requesting a description of services offered by the device.

35. The article of claim 32, wherein the data further includes data, which when accessed by the machine, results in the machine performing, while on the external network, requesting a description of services offered by the device.

36. Machine-accessible information for an intermediary selectively coupling an external network and an internal network embodied in a propagated signal which, when accessed, results in the intermediary performing:

receiving a secure session establishment request by a second device on the external network to establish a secure communication session with a first device on the internal network;

forwarding the secure session establishment request to the first device;

monitoring the internal network for an approval or disapproval acknowledgement by the first device for the secure session establishment request; and

if an approval authentication acknowledgement is monitored, then configuring a first filter rule of the intermediary to allow communication between the first and second devices through the intermediary.

37. The propagated signal of claim 36, wherein the machine-accessible information further includes information, which when accessed, results in the intermediary performing:

receiving a service request from the second device for the first device, the service request having an associated communication port for performing the service;

determining the service request identifies a service advertised by the first device in a device description document; and

configuring a second filter rule to allow communication between the first device and the second device using the associated communication port.